Comments of Electronic Frontier Foundation in Support of Class 21

June 2, 2015

The Electronic Frontier Foundation ("EFF") hereby responds to issues raised in opponents' late-filed written comments of May 19, 2015.

None of the written comments of May 19, 2015, assert that the uses contemplated in Class 21 infringe copyright law. Rather, they seek to block the exemption on the basis of theoretical non-copyright risks and assert that there is no need for the diagnosis and repair aspects of the exemption. Congress and the courts, however, have rejected the application of copyright law to address non-copyright harms, and opponents' factual arguments are unfounded: the record demonstrates both that the non-copyright risks of the exemption are illusory and that the exemption is needed to address concrete and substantial adverse effects on non-infringing diagnosis and repair activities.

I. The Librarian May Not Deny an Exemption on the Basis of Non-Copyright Risks

Section 1201 instructs that the Librarian "shall" create exemptions for any class where "**noninfringing** uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected."[1] The statute provides four specific elements to examine as well as "such other factors as the Librarian considers appropriate" in determining whether this standard is met. Contrary to opponents' claims, the flexibility to consider "other" factors is not a Congressional invitation to restrain noninfringing activities on the basis of the Librarian's assessment of policy questions in such far flung arenas as environmental policy and vehicle safety.

Rather, Congress crafted Section 1201 so that the Librarian would *not* be faced with the task of evaluating competing claims about non-copyright issues. In its original form, the rulemaking standard was to be "whether users of copyrighted works have been, or are likely to be in the succeeding 2-year period, adversely affected… in their ability to make **lawful** uses … of copyrighted works."[2] This language was narrowed so that, in the final version, the consideration is not whether the impeded uses are lawful, but simply whether they are "noninfringing."[3] Congress thus rejected the proposal that the rulemaking would have to evaluate whether non-copyright regulations barred the uses contemplated by a proposed class.

This rulemaking was intended to be a safety valve to ensure that Section 1201 does not overreach its legitimate scope. In jurisdictions that have interpreted Section 1201 liability not to require a nexus with infringement, this rulemaking is the only mechanism that can enforce the traditional contours of copyright law, such as fair use and the idea/expression dichotomy. The Supreme

[1] 17 USC 1201(a)(1)(D) (emphasis added).
[2] H.R. REP. NO. 105-551, pt. 2, at 2-3 (1998) (emphasis added).
[3] 17 USC 1201(a)(1)(D).

Court has explained that these traditional contours are copyright law's "built-in First Amendment accommodations," there to protect freedom of expression.[4] For a noninfringing activity to be restrained by copyright law on the basis of non-copyright risks would be a dramatic departure from established law.[5]

The language, history, and purpose of Section 1201, as well as copyright law's First Amendment contours, dictate that non-copyright risks cannot justify denying an exemption.

II. Contrary to Opponents' Assertions, Safety and Emissions Will Be Improved by Removing the Threat of DMCA Liability

Even if consideration of "non-copyright risks" of granting an exemption were appropriate here, which it is not, such risks are illusory. Auto manufacturers are attempting to create fear, uncertainty, and doubt to maintain their ability to restrain legitimate competition in the vehicle aftermarket.

Far from being harmful of malicious, proponents have pointed out that many of the actual noninfringing uses within the proposed class are specifically directed to improving the environmental impact of vehicle use (e.g. Derive Systems' reprogramming fleets of vehicles or activities of individual ecomodders) and improving safety (e.g. Automatic Labs' "health check" feature to help drivers detect problems and keep cars in good repair and comments of individuals prevented from repairing their own locking systems). This is a continuation of the proven track record of independent tinkerers, who are responsible for dramatically *decreasing* emissions through inventions such as catalytic converters and for saving countless lives via the invention of air bags, retractable seatbelts, roll bars, and other improvements.[6]

Proponents have also introduced specific evidence demonstrating that opponents' speculation about harms is unfounded. The CEO of Derive Systems explained that his company has made over 1.3 million modifications to vehicle software without causing any accidents or even unintended interactions with other ECUs in the vehicle.[7] And contrary to Mr. Douglas' assertion that changes to improve fuel economy "typically increase vehicle air pollution," Derive Systems achieves an average 8-12% reduction in both fuel consumption and emissions.[8] Mr. David Blundell explains well-known avenues available to tinkerers to improve fuel economy without compromising safety or emissions compliance in detail in his June 2, 2015, response to the opponents' late filing.

---

[4] *Golan v. Holder*, 132 S.Ct. 873, 877-78 (2012); *Eldred v. Ashcroft*, 123 S.Ct. 769, 774 (2003).
[5] *See Garcia v. Google, Inc.*, 2015 WL 2343586, at *8 (9th Cir. May 18, 2015) (en banc) (explaining that "threats to life" and "emotional turmoil," while serious, "are untethered from—and incompatible with—copyright and copyright's function as the engine of expression.")
[6] Comments of SEMA in Support of Class 21, at 2-3 (May 1, 2015).
[7] Comments of EFF in Support of Class 21, Appendix A at ¶¶4, 5 (May 1, 2015).
[8] *Id.* at 7.

Rather than seriously challenging proponents' evidence, or introducing concrete evidence of their own, opponents continue to speculate about ways in which hypothetical malicious or negligent actors might cause harm. In no case do they identify any gaps in the other, domain-specific laws designed to address such harms. To the contrary, they reiterate that vehicles are highly-regulated, and identify examples of malicious activity that violate laws against fraud, wiretapping, hacking, and even murder. Such activities are not even covered by the proposed exemption, either because they are not "lawful" modification or because they are not performed by (or on behalf of) the vehicle owner. Moreover, someone interested in bugging, tracking, or sabotaging a car has much easier options than circumventing the computer system.[9] Indeed, many systems can be disabled by a pair of wire-cutters, but no one would argue that we should have a blanket prohibition on their use.

Opponents claim that the exemption would threaten to vehicle owners, but the proposed exemption would have the opposite effect, allowing vehicle owners to inspect their vehicle software for signs of malicious activity, to fix issues they find, and to install improved security mechanisms. Granting the proposed exemption levels the playing field so that people who care about obeying the law can look at and modify vehicle software to protect themselves and others.

Experience with non-vehicular technologies demonstrates that removing Section 1201 as a barrier to innovation helps device owners protect their security and privacy. While vulnerabilities, malware, and bad actors exist regardless of whether law-abiding device owners can circumvent, privacy-respecting custom operating systems and apps often require circumvention to be effective and cannot thrive under a legal cloud of 1201 liability. The popular CyanogenMod custom operating system for Android, which requires an unlocked bootloader, has long included better privacy controls than the stock operating system.[10] Even without a custom operating system, jailbreaking is required in order to use many privacy and security apps,[11] and apps that require jailbreaking tend to practice better respect for user privacy.[12] Developers of privacy technologies such as Tor also work with victims of domestic violence to help them protect themselves from stalkers and abusers.[13] EFF itself publishes digital self-defense guides to empower journalists, activists, and LGBTQ youth to protect their privacy and

[9] Blundell Statement in Support of Class 21 (June 2, 2015), at 4-5.
[10] *Protecting Your Privacy: App Ops, Privacy Guard, and XPrivacy*, XDA Developers (June 11, 2014), http://www.xda-developers.com/protecting-your-privacy-app-ops-privacy-guard-and-xprivacy/ (all URLs last visited June 1, 2015).
[11] Ian Paul, *iPhone Jailbreak: 5 Apps to Control your Privacy*, Tech Hive, http://www.techhive.com/article/250539/iphone_jailbreak_5_apps_to_control_your_privacy.html
[12] Killian Bell, *Jailbreak-Only Apps Respect Your Privacy More Than App Store Apps*, Cult of Mac (February 15, 2014), http://www.cultofmac.com/146456/jailbreak-only-apps-respect-your-privacy-more-than-app-store-apps-report/
[13] Meghan Neal, *Tor Is Being Used as a Safe Haven for Victims of Cyberstalking*, Motherboard (May 9, 2014), http://motherboard.vice.com/read/tor-is-being-used-as-a-safe-haven-for-victims-of-cyberstalking

safety.[14] Vehicle tinkerers should have the same ability to inspect or modify vehicle software so they can protect themselves and others.

III. The Record Demonstrates the Adverse Effects of Prohibition on Legitimate Repair and Diagnosis

Opponents continue to insist that there is no need for the exemption because they have promised to make certain information commercially available. In light of the demonstrated limitations of the Memorandum of Understanding, opponents now seek to rely instead on the Dorgan Letter. When the ASA privately negotiated that agreement with manufacturers, it was criticized for "protecting a monopoly" and "cut[ting] deals for themselves."[15] In addition to the entities that became eventual parties to the MoU, many other organizations considered the Dorgan Letter inadequate, including the American Automobile Association (AAA), Public Citizen, The Consumer Federation of America, Advocates for Highway and Auto Safety, Center for Auto Safety, and the Associated Locksmiths of America,[16] as well as the Tire Industry Association[17] and the Automotive Parts and Service Alliance.[18] The agreement was vague in its promises, with no means for enforcement, and even years later manufacturers were still "refus[ing] to disclose the same information to the independent repair shops, effectively shutting the independents out of the auto-repair market."[19]

The record in this proceeding shows that even today access to needed information is limited. In addition to the ample evidence showing that independent repair shops often cannot match dealer access to needed repair information and documenting that the prices for such information effectively exclude individuals and small independents, we note that one manufacturer flatly refused to sell a license to one witness because he was not associated with a dealership.[20] Another charges $50,000 per year for a license to information about the data coming out of vehicle ECUs (a "data stream" license).[21] Others impose contractual restrictions on licensees of

---

[14] Electronic Frontier Foundation, *Surveillance Self-Defense*, https://ssd.eff.org/; Eva Galperin and Kit Walsh, *New Surveillance Self-Defense Playlist for LGBTQ Youth*, Electronic Frontier Foundation Deeplinks Blog (April 14, 2015), https://www.eff.org/deeplinks/2015/04/new-surveillance-self-defense-playlist-lgbtq-youth

[15] Lisa Greenberg, *Agreement Splinters Groups*, SearchAutoParts.com (December 1, 2002), http://www.searchautoparts.com/abrn/agreement-splinters-groups

[16] *Id.*

[17] Miles Moore, *Repair data pact pleases auto groups*, Tire Business (October 14, 2002), http://www.tirebusiness.com/article/20021014/ISSUE/310149974

[18] John Lypen, *Editor's Report*, Motor (November 2002), available at http://www.motor.com/magazine/pdfs/112002_03.pdf

[19] *Marzulla: The Right to Repair* Act, The Washington Times (May 3, 2009), http://www.washingtontimes.com/news/2009/may/03/the-right-to-repair-act/

[20] Comment of Chris Valasek in Support of Class 21 (June 2, 2015).

[21] *Special OEM License Requirements*, The Equipment and Tool Institute, http://www.etools.org/OEMLicensing/

this information.[22] It bears reiterating, too, that innovators like Derive Systems develop capabilities *beyond* what manufacturers provide to the market at any price.[23]

Under the traditional contours of copyright law, manufacturers have no right to prevent reverse engineering of vehicle software to create competing products and services based on non-copyrightable information. They likewise have no right to enjoin someone from publishing that non-copyrightable information for the benefit of individual vehicle tinkerers or repair professionals, or making other noninfringing uses of vehicle software. It is only the DMCA's prohibition on circumvention that allows manufacturers to restrain competition and innovation in the vehicle aftermarket, pick and choose what information to make available to whom, and charge prohibitive tolls for access to information that could otherwise be lawfully reverse engineered.

Since proponents have established that the prohibition on circumvention is having substantial adverse effects on noninfringing uses of vehicle software for repair, diagnosis, and modification, the proposed exemption should be granted.

Respectfully submitted,

Electronic Frontier Foundation
Kit Walsh
Corynne McSherry
Mitch Stoltz
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
rulemaking-2015@eff.org

Counsel for EFF:
Marcia Hofmann
Law Office of Marcia Hofmann
25 Taylor Street
San Francisco, CA 94102
(415) 830-6664

[22] *Id.*
[23] Comments of EFF in Support of Class 21, Appendix A at ¶1 (May 1, 2015) ("We are able to access and modify ECU software in ways that commercially available tools from Original Equipment Manufacturers (OEMs) can't.")